•	r						Page 1	of 2			
Form PTO-1449 (MODIFIED)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE				SERIAL NO. 09/761,771					
				068398-01	.02						
INE	DESATI	ON DISCLOSURE	CITATION	APPLICANT Virgil D. Gligor et al.							
INF	JKIMA I I	ON DISCLOSURE	CHARON								
				FILING DATE	GROUP ART LINIT						
	(USB SE	everal sheets if nece	 	01/18/200	anasarqued						
	,		U.S. PATE	NT DOCUMENTS				B			
EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB- CLASS	APPRO	PRIATE			
PE							0				
'O	m = 1		FOREIGN PA	TENT DOCUMENTS			•				
711 1 1 E		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB- CLASS	TRANSLATION				
<u> </u>	REF		DATE				YES	NO			
TA IRAD	M.F.										
		OTHER DOCU	MENTS (Including	Author, Title, Date, Pert	inent Pages,	Etc.)					
m	A1 /	A.J. Menezes et al, "Hash Functions and Data Integrity", Handbook of Applied Crytography, Chp 7, pp 223-									
		282; Chp 9, pp 321-383, 1997; CRC Press, Boca Raton									
	A2	Gligor et al, "Object Migration and Authentication", IEEE Transactions on Software Engineering SE-5, vol. 5,									
\sim		pp. 607-611, 1979, IEEE									
0-	А3	NBS FIPS Pub 46, titled "Data Encryption Standard", National Bureau of Standards, U.S. Dept of Commerce									
27		January 1977, pp. 1-18									
00	<u> </u>	NBS FIPS Pub 81, Titled "DES Modes of Operation", National Bureau of Standards, U.S. Dept of Commerce									
1)	A4	pp. 1-17, December 1980									
21		Meyer et al, Cryptography; A New Dimension in Computer Data Security", A Guide For The Design and									
	A5	Implementation of Secure Systems, pp. 69-71, 1982, John Wiley & Sons, 2 nd printing									
		Bellare et al, "A Concrete Security Treatment of Symmetric Encryption", Proceedings of the 38 th Symposium									
n	A6	on Foundations of Computer Science, IEEE, 1997, pp. 394-403									
	A7	C.M. Campbell, "Design and Specification of Cryptographic Capabilities", in Computer Science And The Data									
M		Encryption Standard, (D.K. Brandstad (ed.) National Bureau of Standards Special Publications 500-527									
n	1	U. S. Dept of Commerce, February 1978, pp. 54-66									
n n	A8	Naor et al, "From Unpredictability to Indistinguishability: A Simple Construction of Pseudo-Random Functions									
		From MACs", in Advances in Cryptolog – CRYPTO '98 (LNCS 1462), pp. 267-282, 1998, Springer-Verlag									
2	A9	Goldwasser et al, "Lecture Notes on Cryptography", 1999, Available at									
		http://www.cse.ucsd.edu/users/mihir/papers/gb.pdf									
m	A10	Kohl et al, RFC 1510, The Kerberos Network Authentication Service (V5)", Internet Request For Comments									
		4510									

EXAMINER DATE CONSIDERED

12/7/04

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include any copy of this form with next communication to applicant.

July 17, 2001

	3						Dogo 2	af 2			
Form PTO-1449		U.S. DEPARTMENT OF COMMERCE		ATTY, DOCKET NO.		Page 2 of 2 SERIAL NO.					
(MODIFIED)		PATENT AND TRADEMARK OFFICE		068398-0102		09/761,771					
				APPLICANT							
INF	ORMATI	ON DISCLOSURE	CITATION	Virgil D. Gligor et al.							
				FILING DATE	GROUP ART UNIT						
(Use several sheets if necessary)				01/18/20	Unassigned						
			U.S. PATER	IT DOCUMENTS							
EXAMINER INITIAL	REF	DOCUMENT	DATE	NAME	CLASS	SUB- CLASS	FILING DATE				
		NUMBER					IF APPROPRIATE				
Q E JC,				**		 					
5 ~	43		FORFIGN PAT	ENT DOCUMENTS		1	I				
1 100		DOCUMENT	T GREIONT AT	EIII BOOOMEIII	Т	SUB- CLASS	TRANSLATION				
JIIL.	₽F F	DOCUMENT NUMBER	DATE	COUNTRY	CLASS		YES	NO			
FRAT & TRAS								,			
	<u></u>	OTHER DOCU	MENTS (Including A	Author, Title, Date, Pe	rtinent Pages,	Etc.)		L			
		Petrank et al, "CBC	MAC for Real-Time D	ata Sources:, Manuscript Available at							
n	A11	http://www.cs.technion.ac.il/~erez/publications.html, 1999									
m	A12	Jueneman et al, "Message Authentication with Manipulation Detection Codes", Proc. Of the IEEE Symp. on									
		Security and Privacy, Oakland, CA, pp. 33-54, 1983, IEEE Computer Society									
		Stubblebine et al, "On Message Integrity in Cryptographic Protocols", Proceedings of the 1992 IEEE Computer									
2	A13	Society Symposium on Research in Security and Privacy, pp. 85-104, 1992, IEEE Computer Society Press									
		Kohl et al, "The use of Encryption in Kerberos for Network Authentication", Advances in Cryptology-CRYPTO									
n	A14	1989, (LNCS 435), pp. 35-43, 1990, Digital Equip. Corp.									
1	A15	D. E. Knuth, "The Art of Computer Programming – Volume 2: Seminumerical Algorithms", 1981, (2 nd ed.)									
3	AIS	Chapter 3, pp. 1-110, Addison-Wesley									
					·						
		Prom									
		TECEIVED									
		JUL 1 9 2001									
		Technology									
		Technology Center 2100									
	,										
EXAMINER		· · · · · · · · · · · · · · · · · · ·		DATE CONSIDER	RED ,						

* EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include any copy of this form with next communication to applicant.

July 17, 2001

4

U.S. DEPARTMENT OF COMMERCE ATTY. DOCKET NO. Form PTO-1449 SERIAL NO. 068398-0102 (MODIFIED) PATENT AND TRADEMARK OFFICE 09/761,771 APPLICANT INFORMATION DISCLOSURE CITATION Virgil D. Gligor et al. **GROUP ART UNIT** LING DATE 01/18/2001 2131 (Use several sheets if necessary) **DOCUMENTS** FILING DATE DOCUMENT SUB-**EXAMINER** DATE NAME CLASS REF **CLASS** INITIAL NUMBER APPROPRIATE FOREIGN PATENT DOCUMENTS TRANSLATION DOCUMENT SUB-**CLASS** DATE COUNTRY REF NUMBER CLASS YES NO OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.) Gligor Virgil D. and Donescu Pompiliu. "Fast Encryption and Authentication; XCBC Encryption and XECB Α1 Authentication Modes." VDG Inc. 27 October 2000. Pages 1 - 30. http://citeseer.nj.nec.com/cs. Rogaway, Phillip, "Comments to NIST Concerning AES Modes of Operation: PMAC: A Parallelizable Message Authentication Code." Univ. of CA at Davis and Chiang Mai Univ. Thailand. 16 October 2000. Pages 1 – 6. **A2** n http://citeseer.nj.nec.com/cs>. Proceedings IEEE Symposium on Security and Privacy. Jueneman, R.R., Matyas, S.M., and Meyer, C.H. А3 "Message Authentication with Manipulation Detection Codes." Pages 33 – 54, 25 April 1983. DATE CONSIDERED **EXAMINER** 12/7/64 EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include any copy of this form with next communication to applicant.